Mobile Connect for iOS 3.0 User Guide

SONICWALL®

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2014 Dell Inc.

Trademarks: SonicWALL™, Aventail™, SonicWALL Mobile Connect™, and all other SonicWALL product and service names and slogans are trademarks of SonicWALL, LLC, a wholly owned subsidiary of Dell.

2014 – 3 P/N 232-002406-00 Rev. A

Table of Contents

How Mobile Connect Works 5
Prerequisites 5
- Apple Product Support 6
- Dell SonicWALL Appliance Support 6
- What's New in This Release? 6
- Required Network Information 7

Installing Mobile Connect 8
Using Mobile Connect 9
- Create a Connection 9
- Connect to the Mobile Connect Server 13
- Configure Mobile Connect Settings 15
- URL Control Syntax and Parameters 17
- Bookmarks 21
- Files 23
- Configure Connect on Demand 29
- Configure Trusted Network Detection 33
- To Use the iPhone Configuration Utility with Mobile Connect 34

Monitor Mobile Connect 37
Troubleshoot Mobile Connect 38

Using Mobile Connect for iOS

SonicWALL Mobile Connect for iOS is an app for Apple iPhone, iPod touch, and iPad that enables secure, mobile connections to private networks protected by Dell SonicWALL security appliances.

How Mobile Connect Works

Modern business practices increasingly require that users be able to access any network resource (files, internal websites, etc.), anytime, anywhere. At the same time, ensuring the security of these resources is a constant struggle. While most users are aware that they must take care to protect computers from network security risks, this security awareness does not always extend to mobile devices like the iPhone, iPod touch and iPad. And yet, mobile devices are increasingly subject to security attacks. Furthermore, mobile devices often use insecure, untrusted, public Wi-Fi hotspots to connect to the Internet. It is therefore a challenge to provide secure, mobile access while still guarding against the inherent security risks of using mobile devices.

The SonicWALL Mobile Connect app for iPhone, iPod touch, and iPad provides secure, mobile access to sensitive network resources. Mobile Connect establishes a Secure Socket Layer Virtual Private Network (SSL VPN) connection to private networks that are protected by Dell SonicWALL security appliances. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

After installing SonicWALL Mobile Connect from the App Store, to get started with Mobile Connect:

1. Ensure the Dell SonicWALL SRA or firewall appliance that will be used by Mobile Connect to the network is connected.
2. Configure Network Information (server name, username, password, etc.).
3. Mobile Connect establishes a SSL VPN tunnel to the Dell SonicWALL security appliance.
4. You can now access resources on the private network. All traffic to and from the private network is securely transmitted over the SSL VPN tunnel.

Prerequisites

The following sections describe prerequisites for SonicWALL Mobile Connect:

- “**Apple Product Support**” on page 6
- “**Dell SonicWALL Appliance Support**” on page 6
- “**Required Network Information**” on page 7

Apple Product Support

SonicWALL Mobile Connect is supported on the following devices:

- iPhone 5s – running iOS 7 or higher
- iPhone 5c – running iOS 7 or higher
- iPhone 5 – running iOS 6 or higher
- iPhone 4S – running iOS 6 or higher
- iPhone 4 – running iOS 6 or higher
- iPhone 3GS – running iOS 6 or higher
- iPad Air (5th generation) – running iOS 7 or higher
- iPad (4th generation) – running iOS 6 or higher
- iPad (3rd generation) – running iOS 6 or higher
- iPad 2 – running iOS 6 or higher
- iPad mini – running iOS 6 or higher
- iPad (4th generation – running iOS 6 or higher
- iPad (3rd generation) – running iOS 6 or higher
- iPad 2 – running iOS 66 or higher
- iPad mini (2nd generation) – running iOS 7 or higher
- iPad mini – running iOS 6 or higher
- iPod touch (4th generation or later) – running iOS 6 or higher

Dell SonicWALL Appliance Support

SonicWALL Mobile Connect is a free app, but requires a concurrent user license on one of the following Dell SonicWALL solutions in order to function properly:

- Dell SonicWALL firewall appliances including the TZ, NSA, E-Class NSA running SonicOS 5.8.1.0 or higher
- Dell SonicWALL SRA appliances running 5.5 or higher
- Dell SonicWALL Aventail E-Class Secure Remote Access (SRA) appliances running 10.5.4 or higher

What's New in This Release?

The following features, some of which are specific to E-Class SRA appliances or SMB SRA appliances and Next Generation Firewalls, have been added in Mobile Connect 3.0:

- **iOS 7 Redesign** – Apple introduced many new UI changes and design paradigms in iOS 7 that require apps to be fundamentally redesigned for iOS 7, with any changes then adapted to iOS 6. Mobile Connect has been completely redesigned to be simpler and more useful according to the design principles of iOS 7.

  Mobile Connect 3.0 has a new app icon, splash screen, and look and feel when run on iOS 7. The **Connect**/**Disconnect** button has been replaced with an **On**/**Off** switch, matching the same VPN controls in the Settings app. On iOS 6 Mobile Connect retains its original look and feel.
- **File Bookmarks** – Mobile Connect 3.0 working with SRA 7.5 firmware introduces secure mobile access to files. Granular policy controls can be configured to allow or deny other iOS apps and features to use each file. Policies include control over whether a file may be printed, securely cached, copied to the clipboard, or opened in a third party app. Files

Bookmarks are displayed after the VPN is connected. Selecting a Files bookmark checks and enforces the server policy, securely downloads the file, and displays it within the Mobile Connect app. Bookmarks to folders or file share root directories can also be created to allow for directory navigation.

At this time File bookmarks are supported only in SMB SRA appliances running SRA 7.5 firmware. File bookmark support in the E-Class SRA and Next Generation Firewalls is expected in a future release.

E-Class SRA Features

- **Credential Caching** – Users may now cache their username and password credentials to reduce the burden of managing their credential identities to gain access. This feature requires 10.7.x E-Class SRA firmware.
- **Network Awareness** – VPN connections can be configured to detect whether the user is remote or on premise and control the VPN connection accordingly. This feature requires 10.7.x E-Class SRA firmware.
- **IPv6 Phase I Support** – VPN connections can connect to SRA EX appliances via IPv6 and access IPv6 resources over the VPN. This feature requires 10.7.x E-Class SRA firmware.
- **TLSv1.1/1.2 Support** – This feature requires 10.6.4+ or 10.7.x E-Class SRA firmware.

SMB SRA & Next Generation Firewall Features

- **Client Certificate Authentication and iOS VPN On Demand Support** – iOS supports VPN On Demand for networks that use certificate-based authentication. VPN On Demand automatically establishes a secure VPN connection when needed. Client certificate configuration is now available for SRA appliance connections. If a client certificate is selected, VPN On Demand settings may be configured as well.
- **Compression** – Traffic over the VPN tunnel is compressed using the LZ4 algorithm when connected to a server that supports compression and has it enabled for the tunnel. A Compression row displaying the overall compression ratio is shown on the Monitor tab if compression is enabled. This feature requires 7.5 SRA firmware.
- **End Point Control** – End Point Control policy checking is performed before establishing the VPN connection established. Mobile Connect supports the following attributes:
  - Application
  - Directory name
  - File name
  - Equipment ID
  - iOS version.

  This feature requires 7.5 SRA firmware.

Required Network Information

To use Mobile Connect, you will need the following information from your network administrator or IT Support:

- Server name or address – This is either the IP address or URL of the SSL VPN server that you will connect to.
- Username and password – Typically, you will be required to enter your username and password, although some connections may not require this.
- Domain name – The domain name of the SSL VPN server. Mobile Connect may be able to automatically determine this when it first contacts the server, or there may be multiple domains that can be selected.

DNS Domain Settings on Appliances

Before Mobile Connect users will be able to access the private network, the network administrator must configure the DNS Domain on the Dell SonicWALL appliance. When the Mobile Connect user accesses a URL on the private network, the configured DNS domain is used to resolve the hostname lookup. For public domains that do not match the configured DNS domain, the DNS server for the Wi-Fi or cellular network is used.

Note The Mobile Connect user does not need to perform any configuration tasks related to DNS. The following information is for SonicWALL network administrators.

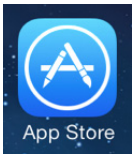
The DNS Domain configuration process varies, depending on the type of Dell SonicWALL appliance being used:

- **Dell SonicWALL firewall appliances** – On the **SSL VPN > Client Settings** page, enter the DNS domain name in the **DNS Domain** field.
- **Dell SonicWALL SRA appliances** – The DNS domain can be configured either globally, at the group level, or at the individual user level:
  - Global level: On the **Network > DNS** page, enter the DNS domain name in the **DNS Domain** field.
  - Group level: On the **Users > Local Groups** page, click the edit icon for the group. Click on the **NX Settings** tab and enter the DNS domain the **DNS Domain** field.
  - User level: On the **Users > Local Users** page, click the edit icon for the user. Click on the **NX Settings** tab and enter the DNS domain the **DNS Domain** field.
- **Dell SonicWALL E-Class SRA appliances** – The DNS domain can be configured either globally or for specific IP address pools:
  - Global level: From the main navigation menu in the E-Class SRA Management Console (AMC), click **Network Settings**. In the **Name resolution area**, click **Edit**. The **Configure Name Resolution** page appears. Enter the DNS domain name in the **Search domains** field.
  - IP address pool level: From the main navigation menu in the AMC, click **Services**. Under **Access services**, in the Network tunnel service area, click **Configure**. The **Configure Network Tunnel Service** page appears. Click the name of the IP address pool you want to edit. The **Configure IP Address Pool** page appears. To the right of the **Advanced** heading, click the arrow icon. Select the **Customize default settings** checkbox and enter the DNS domain name in the **Search domains** field.

Installing Mobile Connect

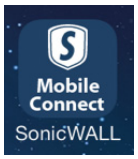
SonicWALL Mobile Connect is installed through the Apple App Store.

1. On your iPhone, iPod touch, or iPad, tap the App Store icon.



2. Go to the **Search** tab, enter **SonicWALL Mobile Connect**, and tap **Search**.
3. In the search results, select **SonicWALL Mobile Connect**.

4. Tap **Free** and then **Install**. The app will install on your device. When installation is complete, the SonicWALL Mobile Connect icon will appear on your device.



Note If you encounter an error when attempting to download SonicWALL Mobile Connect, please see iTunes Store Customer Support, where you can find troubleshooting procedures and instructions on how to report the issue using your iTunes account: http://www.apple.com/support/itunes/

Using Mobile Connect

The following sections describe how to use SonicWALL Mobile Connect:

- "**Create a Connection**" on page 9
- "**Connect to the Mobile Connect Server**" on page 13
- "**Configure Mobile Connect Settings**" on page 15
- "**Configure Connect on Demand**" on page 29
- "**To Use the iPhone Configuration Utility with Mobile Connect**" on page 34

Create a Connection

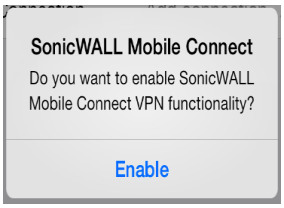
The process of creating a Mobile Connect connection is slightly different depending on which type of Dell SonicWALL appliance you are connecting to.

The following sections describe how to create a connection:

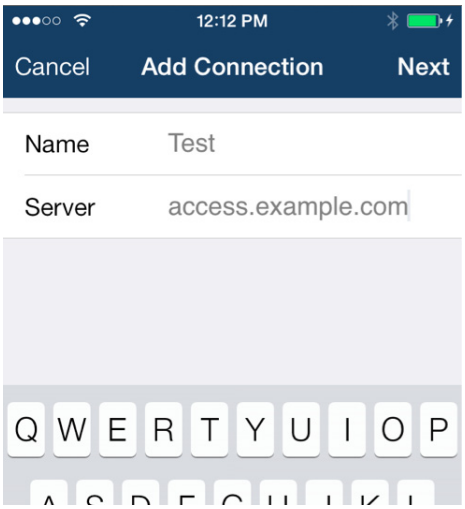
- "**Create a Connection to Dell SonicWALL Firewall and SRA Appliances**" on page 9
- "**Create a Connection to Dell SonicWALL E-Class SRA Appliances**" on page 12

Create a Connection to Dell SonicWALL Firewall and SRA Appliances

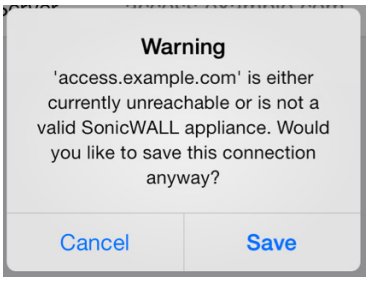
1. The first time you launch Mobile Connect, you will be prompted to enable VPN functionality. Tap **Enable**.



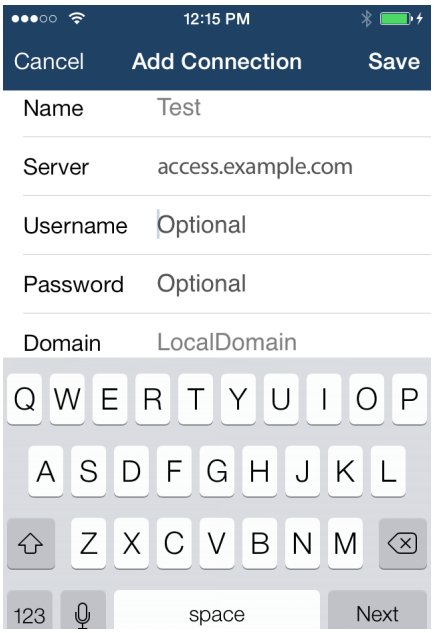
2. You will then be presented with the screen to begin your first connection to the Dell SonicWALL firewall or appliance. Tap **Add connection**.
   - **Name**: Enter a descriptive name for the connection.
   - **Server**: Enter the URL or IP address of the server.



3. Tap **Next**. Mobile Connect will then attempt to contact the Dell SonicWALL appliance. If Mobile Connect successfully contacts the appliance, the server connection is added to the list of saved connects on the Connections screen.
4. If the attempt fails, a warning message will display, asking if you want to save the connection. Verify that the server address or URL is spelled correctly, and then tap **Save**.

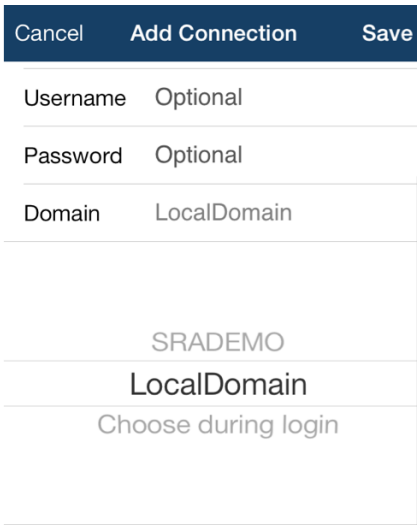

Warning
'access.example.com' is either currently unreachable or is not a valid SonicWALL appliance. Would you like to save this connection anyway?
Cancel
Save

5. If Mobile Connect successfully contacts the server, you will be prompted to optionally enter your **Username** and **Password** (unless the server does not require this information). Enter your Username and Password, and then scroll down to the **Domain** field.



Note If the screenshots above do not match what is displayed on your device, you are connecting to a Dell SonicWALL E-Class SRA appliance. Proceed to "**Create a Connection to Dell SonicWALL E-Class SRA Appliances**" on page 12.

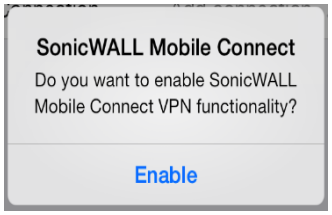
The **Domain** field is auto-populated with the default domain from the server. To select a different domain, tap **Domain** to display a drop-down menu of the available options, select the correct domain.



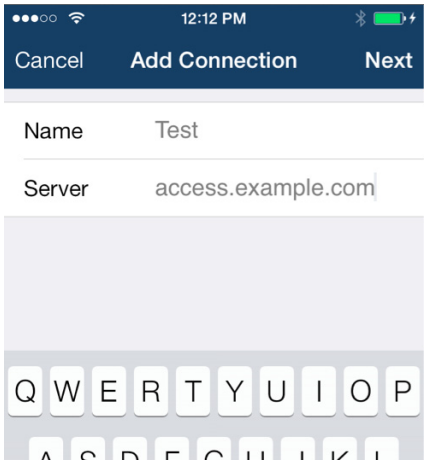
6. Tap **Save**, which displays the Connections window where you select the server connection.

Create a Connection to Dell SonicWALL E-Class SRA Appliances

1. The first time you launch Mobile Connect, you will be prompted to enable VPN functionality. Tap **Enable**.

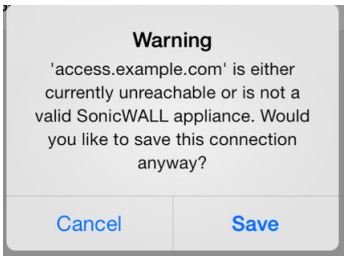


2. You will then be presented with the screen to begin your first connection. Tap **Add connection**.
   - **Name**: Enter a descriptive name for the connection.
   - **Server**: Enter the URL or IP address of the server.



3. Tap **Next**. Mobile Connect will then attempt to contact the Dell SonicWALL appliance. If Mobile Connect successfully contacts the appliance, the server connection is added to the list of saved connects on the Connections screen.

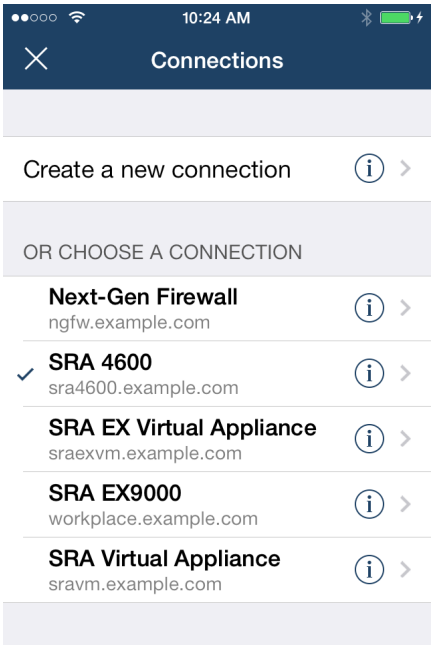
   If the attempt fails, a warning message will display, asking if you want to save the connection.


Warning
'access.example.com' is either currently unreachable or is not a valid SonicWALL appliance. Would you like to save this connection anyway?
Cancel
Save

4. Before tapping **Save**, verify that the server address or URL is spelled correctly. Clicking **Save** adds the server connection to the list of saved connections on the Connections screen.

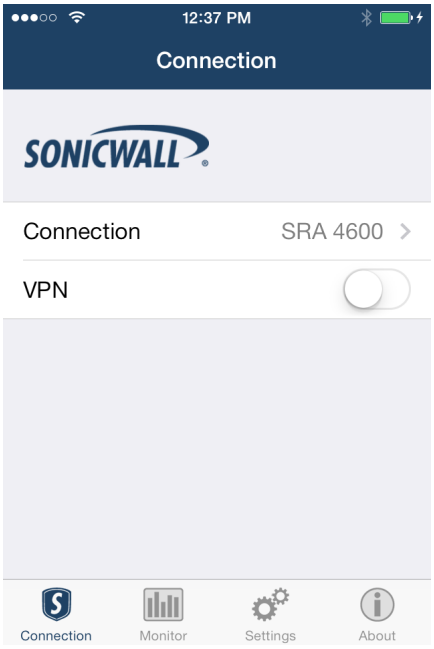
Connect to the Mobile Connect Server

After you save a new connection, the list of all configured connections displays.



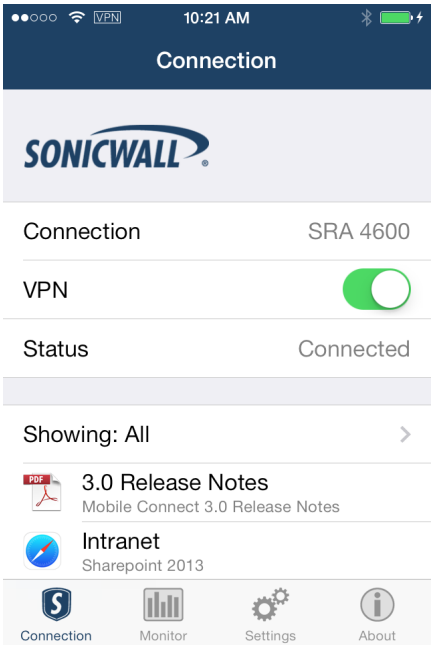
To establish a Mobile Connect session, perform the following tasks:

1. Tap the connection in the list that you want to initiate. The Connection page displays. Enable the **VPN** by tapping the switch.



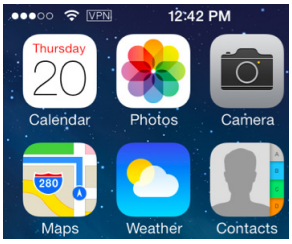
2. Enter your username and password if prompted (depending on whether the appliance you are connecting to allows for saving usernames and passwords), and tap **Login**.

3. When the connection is successfully established, the **Status** row changes to **Connected** and the **VPN** switch will be on.



Any bookmarks defined for the portal are displayed below the **Status** row. Launch a bookmark by tapping on it.

4. Press the Home button on your iPhone, iPod touch, or iPad to display its home screen. You can now navigate to other apps to access your Intranet network. The status bar at the top of the iPhone, iPod touch or iPad displays a VPN icon to indicate that the Mobile Connect session is still connected.

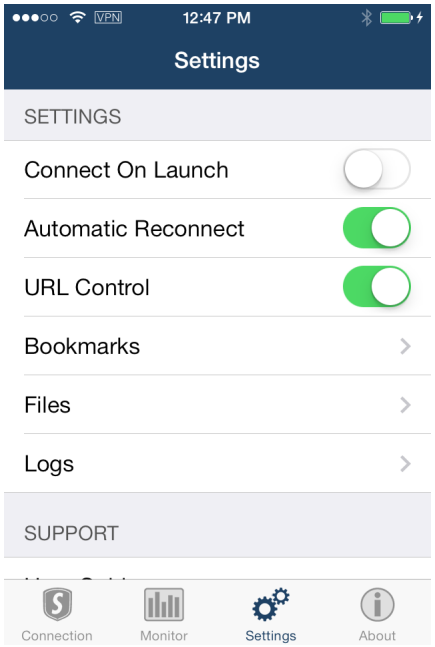


If the VPN connection is interrupted, the VPN icon will disappear and you will no longer be able to access the Intranet network. This can happen if your device's connection transitions from Wi-Fi to cellular or to another network type.

Return to Mobile Connect to reestablish the connection. Optionally, you can configure the **Automatic Reconnect** option on the **Settings** tab to have Mobile Connect automatically attempt to reestablish interrupted connections.

Configure Mobile Connect Settings

SonicWALL Mobile Connect provides several settings for connection and logging options. The Settings tab also provides Support information, which includes a User Guide and device, connection, and server information.



The following options are controlled from the Settings tab:

- **Connect on Launch** - Sets Mobile Connect to automatically initiate a connection to the last-used profile when the app is launched.
- **Automatic Reconnect** - Sets Mobile Connect to automatically attempt to reconnect if the connection is lost. The SSL VPN connection can be disrupted when your device's connection transitions to a different network type (for example, from Wi-Fi to cellular). This setting lets applications rely on a sustained VPN connection. There is no limit on the amount of time it takes to reconnect.
- **URL Control** - Allows other mobile applications to pass action requests using special URLs to Mobile Connect. These action requests can create VPN connection entries and connect or disconnect VPN connections. For example, another application can launch Mobile Connect, access internal resources as needed, and then disconnect by using the mobileconnect:// or sonicwallmobileconnect:// URL scheme. Some common examples of URL Control are:

  Add profile: **mobileconnect://addprofile**[/]**?name=***ConnectionName***&server=***ServerAddress*[**&***Parameter1***=***Value***&***Parameter2***=***Value*...]

  Connect: **mobileconnect://connect**[/]**?[name=***ConnectionName*|**server=***ServerAddress*][**&***Parameter1***=***Value***&***Parameter2***=***Value*...]

  Disconnect: **mobileconnect://disconnect[/]**

  Additional information about URL Control is provided in "**URL Control Syntax and Parameters**" on page 17.

- **Bookmarks** - Displays centrally configured shortcuts, called bookmarks, to VPN resources such as URLs, Outlook Web Access, and iOS applications. These bookmarks, which are displayed on the main Connection tab when the VPN is connected, provide one-touch access to frequently used applications.

  If using an SRA appliance, pulling down the Connection screen and releasing it refreshes the bookmarks. Mobile Connect supports Remote Desktop options like screen size and enable/disable audio as long as both the server bookmark and third party iOS application support the option.

  Note Bookmarks are supported on SRA appliances only when running 7.5 or higher and Next Generation Firewall appliances running SonicOS 5.9.0.2 and higher.

  Additional information about bookmarks is provided in "**Bookmarks**" on page 21.

- **Files** – Deletes all cached files that have been downloaded and stored on the device. Note that cached files are encrypted on the device for added security.

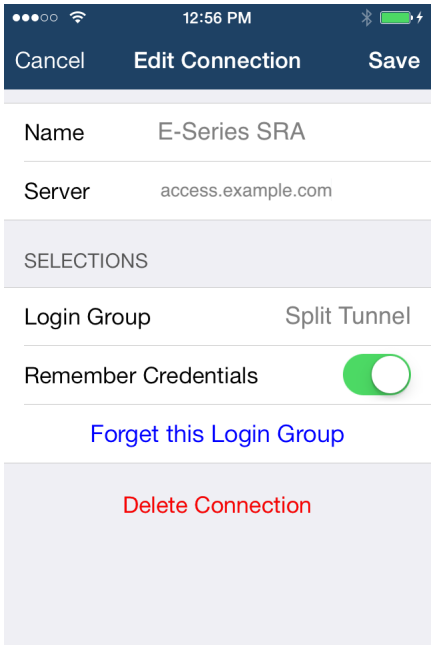
  Note Files are supported on SMB SRA appliances only when running 7.5 or higher and not supported on appliances running SonicOS.

  Additional information about Files is provided in "**Files**" on page 23.

- **Logs** - Serves two purposes:
  - Enables full debug log messages of Mobile Connect activity. Leave this section disabled unless instructed to enable it by Dell SonicWALL Support staff.
  - Deletes all log files that have been saved on the device.

E-Class SRA Settings

Two additional options can be modified for connections to Dell SonicWALL E-Class SRA appliances. To view these options, go to the **Connection** tab and tap the **Connection** line to display the list of connections. Tap the info indicator ⓘ › to the left of the connection you want to modify. The **Edit Connection** window displays.



The following options can be configured:

- **Remember Credentials** - Enables saving of user authentication credentials for the VPN connection. This is disabled by default and can be controlled by the E-Series SRA server setting.
- **Forget this Login Group** - Mobile Connect remembers the Login Group that you specified when configuring the connection. To change to a different Login Group, tap **Forget this Login Group**. The next time you connect to the server, you will be prompted to select a new Login Group.

Note If these options are not displayed, then you are connecting to either a Dell SonicWALL firewall or SRA appliance.

The **Support** section of the Settings tab provides the following support information:

- **User Guide** - Displays the SonicWALL Mobile Connect User Guide.
- **Device Information** - Displays information about the iOS device, Wi-Fi connection, Cellular connection, Bluetooth connection, and DNS servers.
- **Email Logs** - Creates an email to send the Mobile Connect log files to Dell SonicWALL Support staff. Tap **Send** to send the email.

URL Control Syntax and Parameters

This section provides the full set of URL parameters for the URL Control feature. URL Control currently supports the `addprofile`, `connect`, and `disconnect` commands. Callback URLs are also supported.

Add Profile Command

The `addprofile` command requires either the name or server parameter, and accommodates both. All other parameters are optional. When the URL is opened in Mobile Connect, all of the parameters included in the URL are saved in the connection entry associated with that `name` and `server`.

Syntax:

`mobileconnect`**`://addprofile[/]?name=`***`ConnectionName`***`&server=`***`ServerAddress`***
`[`**`&`***`Parameter1`***`=`***`Value`***`&`***`Parameter2`***`=`***`Value...`***`]`

Following are examples of the `addprofile` command:

```
mobileconnect://addprofile/?name=Example&server=vpn.example.com

sonicwallmobileconnect://addprofile/?name=Example&server=vpn.example.com

mobileconnect://addprofile?name=Example%202&server=vpn.example.com

mobileconnect://addprofile?name=vpn.example.com

mobileconnect://addprofile?server=vpn2.example.com

mobileconnect://addprofile?name=SRA%20Connection&server=sslvpn.example.com
&username=test&password=password&domain=LocalDomain&connect=1

mobileconnect://addprofile?name=EX%20Connection&server=workplace.example.com
&username=test&password=password&realm=Corp&connect=1
```

Note All appropriate characters in values of parameters used in URLs are required to be URL encoded. For instance, to match a space, enter %20.

Add Profile Command Parameters

Command Parameter	Description
`name`	The unique name of the VPN connection entry that will be created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
`server`	The domain name or IP address of the Dell SonicWall appliance in which you wish to connect. For example: `vpn.example.com`
`username`	**Optional**: The username used in the VPN connection.
`password`	**Optional**: The password used in the VPN connection.
`realm`	**Optional**: The realm used in the VPN connection profile. Applies to EX series connections only.
`domain`	**Optional**: The domain used in the VPN connection profile. Applies to SRA and UTM connections only.
`sessionid`	**Optional**: The session ID or Team ID used for authentication.
`connect`	**Optional**: If presented and the value is non-null, the connection will be initiated if the profile was successfully added.
`callbackurl`	**Optional**: The callback URL is be opened by Mobile Connect after the add profile command has been processed. See “**Callback URL**” on page 20 for full details of the callback URL syntax and options.

Connect Command

The `connect` command is used to easily establish VPN connections. Connection information can be embedded in the URLs and they can be provided to users for easy setup and configuration. In addition, a callback URL can be provided that Mobile Connect will open after the connection attempt is completed, making it possible for other applications to initiate VPN connections in a seamless manner.

Syntax:

`mobileconnect://connect[/]?[name=`*`ConnectionName`*`|`**`server=`***`ServerAddress`***`]`
`[`**`&`***`Parameter1`***`=`***`Value`***`&`***`Parameter2`***`=`***`Value...`***`]`

Following are examples of the `mobileconnect` command:

```
mobileconnect://connect/?name=Example

sonicwallmobileconnect://connect/?name=Example

mobileconnect://connect?name=Example

mobileconnect://connect?server=vpn.example.com

mobileconnect://connect?name=Example%202&server=vpn.example.com

mobileconnect://
connect?name=SRA%20Connection&server=sslvpn.example.com
&username=test&password=password&domain=LocalDomain

mobileconnect://
connect?name=EX%20Connection&server=workplace.example.com
&username=test&password=password&realm=Corp
```

Connect Command Parameters

Command Parameter	Description
`name`	The unique name of the VPN connection entry that will be created and appear in the Mobile Connect Connections list. Mobile Connect accepts the name only if it is unique. Letters are case sensitive.
`server`	The domain name or IP address of the Dell SonicWall appliance in which you wish to connect. For example: `vpn.example.com`
`username`	**Optional**: The username used in the VPN connection.
`password`	**Optional**: The password used in the VPN connection.
`realm`	**Optional**: The realm used in the VPN connection profile. Applies to EX series connections only.
`domain`	**Optional**: The domain used in the VPN connection profile. Applies to SRA and UTM connections only.
`sessionid`	**Optional**: The session ID or Team ID used for authentication.
`connect`	**Optional**: If presented and the value is non-null, the connection will be initiated if the profile was successfully added.
`callbackurl`	**Optional**: The callback URL is opened by Mobile Connect after the connect command has been processed. See “**Callback URL**” on page 20 for full details of the callback URL syntax and options.

Disconnect Command

The `disconnect` command is used to disconnect an active connection. In addition, a callback URL can be provided that Mobile Connect will open after the connection is disconnected, which makes it possible to return to the calling app. If there is no active VPN connection, the command is ignored.

Syntax:

```
mobileconnect://disconnect[/]
mobileconnect://disconnect[/]?[callbackurl=<callbackurl>]
```

Following are examples of the disconnect command:

```
mobileconnect://disconnect
```

```
mobileconnect://disconnect/
```

```
sonicwallmobileconnect://disconnect
```

```
mobileconnect://
disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%
26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

```
sonicwallmobileconnect://
disconnect?callbackurl=customapp%3A%2F%2Fhost%3Fstatus%3D%24STATUS%24%
26login_group%3D%24LOGIN_GROUP%26error_code%3D%24ERROR_CODE%24
```

Disconnect Command Parameters

Command Parameter	Description
`callbackurl`	**Optional**: The callback URL is opened by Mobile Connect after the disconnect command has been processed. See "**Callback URL**" on page 20 for full details of the callback URL syntax and options.

Callback URL

While invoking Mobile Connect using a URL, a third party application can include a callback URL that is called by Mobile Connect once it completes the requested action. The callback URL value may also contain special tokens that will be evaluated and dynamically replaced by Mobile Connect to provide additional status and connection information back to the app that is opened by the callback URL. Tokens are evaluated in place, in the same order in which the tokens were specified.

To ensure that it functions properly, the base callback URL format should be RFC 1808 compliant and should be able to be launched independently of Mobile Connect. For example it should launch through a web page or iOS web clip.

```
URL: <scheme>://<net_loc>/<path>;<params>?<query>#<fragment>
```

Note

The value of `callbackurl` must also be properly URL encoded to ensure that Mobile Connect can process the callback URL correctly.

Dynamic Tokens Supported by the Callback URL

Dynamic Token	Description
`$ERROR_MESSAGE$$`	The string value of the error message from the failed connection attempt.
`$LOGIN_GROUP$`	The string value of the authentication login group or realm. Applies to EX series connections only.
`$COMMUNITY$`	The string value of authentication community. Applies to EX series connections only.
`$ZONE$`	The string value of EPC zone. Applies to EX series connections only.
`$TUNNEL_IP$`	The string value of the Mobile Connect IPv4 client address.
`$TUNNEL_MODE$`	One of split, split-nonlocal, redirectall, or redirectall-nonlocal depending on the tunnel mode. Applies to SRA and UTM connections only.
`$ESP_ENABLED`	Yes, or no depending on if ESP is enabled. Applies to SRA and UTM connections only.

Note

Any number of tokens from the table above can be specified.

Following are examples using the callback URL:

Callback URL

```
customapp://host?status=$STATUS$&login_group=$LOGIN_GROUP&
error_code=$ERROR_CODE$
```

Full URL with URL Encoded Callback URL Value

```
mobileconnect://connect?sessionid=<teamid>&callbackurl=customapp%3A%2F%
2Fhost%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%
26error_code%3D%24ERROR_CODE%24
```

Callback URL

```
myapp://callback?status=$STATUS$&login_group=$LOGIN_GROUP&
error_code=$ERROR_CODE$
```

Full URL with URL Encoded Callback URL Value

```
mobileconnect://connect?sessionid=<teamid>&callbackurl= myapp%3A%2F%
2Fcallback%3Fstatus%3D%24STATUS%24%26login_group%3D%24LOGIN_GROUP%
26error_code%3D%24ERROR_CODE%24
```

Callback URL

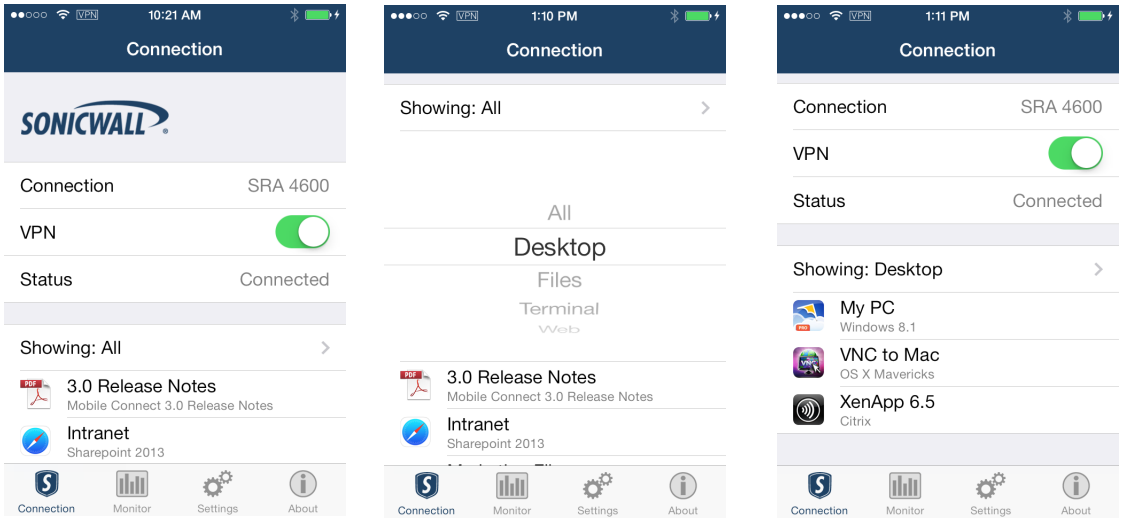
```
http://server/example%20file.html
```

Full URL with URL Encoded Callback URL Value

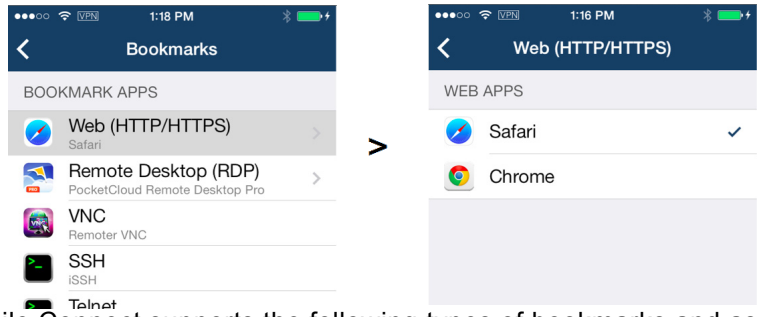
```
mobileconnect://connect?callbackurl=http%3A%2F%2Fserver%2Fexample%2520file.html
```

Bookmarks

When there are more than five bookmarks, the bookmarks can be filtered by selecting the **Showing: <*bookmark type*>** row that is displayed when there are more than five bookmarks lets you filter long lists of bookmarks by type. Select the type of bookmarks to display or select **All** to display all bookmarks.



Selecting a bookmark for an app that is not installed will prompt you to install the app. Apps referenced by bookmarks also can be installed at any time using the Settings > Bookmarks tab. In addition to installing apps for bookmarks, the Settings > Bookmarks tabs is also used to select and install apps for bookmarks that support multiple third party apps. For example, you might select Safari or Google Chrome for a Web bookmark.



Mobile Connect supports the following types of bookmarks and associated apps.

Note

In Mobile Connect for iOS 3.0, only Web and Desktop bookmarks are supported on the Dell SonicWALL EX series SRA appliances.

Desktop Bookmarks:

Portal name: Terminal Services (RDP – ActiveX), Terminal Services (RDP – Java) Internal type: RDP5ActiveX, RDP5Java

RDP bookmark types attempt to launch with the associated RDP application, as configured in the Settings tab.

	iOS Version
Wyse PocketCloud Pro	2.3.211
2X Client RDP/Remote Desktop	11.0.1872
Remote RDP Lite	—
Remote RDP	—
Remote RDP Enterprise	—

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters will vary based on the application. For example:

- Wyse PocketCloud Pro does not support the “connect to console” option
- 2X Client does not accept screen resolution settings on iOS

Portal name: Virtual Network Computing (VNC)
Internal type: VNC

VNC bookmark types attempt to launch with the associated VNC application as configured in the Settings tab.

	iOS Version
Wyse PocketCloud Pro	—
android-vnc-viewer	—
Remoter VNC	4.5.04

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters varies based on the application.

Portal name: Citrix Portal (Citrix)
Internal type: Citrix, Citrix_https

Citrix bookmark types will attempt to launch with the associated Citrix application.

	iOS Version
Citrix Receiver	5.8.3

Additional details such as screen resolution should be provided to the client. However, support for passing such parameters will very based on the application.

Web Bookmarks:

Portal name: Web (HTTP), Secure Web (HTTPS), External Web Site
Internal type: HTTP, HTTPS, URL, URL_https

These bookmarks will launch in an associated web browser and the provided 'Name or IP Address' (HostID) will be passed as the parameter to display in the browser..

	iOS Version
Any Browser	—
Safari	Yes
Google Chrome	33.0.1750.14

Portal name: Mobile Connect
Internal type: MC

Mobile Connect bookmark type will rely fully on the OS to determine and launch the proper application. The bookmark is expected to be properly configured for launch. The Mobile Connect app will attempt to launch it as is. (for example, telnet://server)

Terminal Bookmarks:

In Mobile Connect for iOS 3.0, Dell SonicWALL E-Class SRA appliances do not support Terminal bookmarks.

Portal name: Telnet, Secure Shell Version 1 (SSHv1), Secure Shell Version 2 (SSHv2)
Internal type: Telnet, SSH, SSHv1

	iOS Version
ConnectBot	—
iSSH	5.7.1

ConnectBot notes: Proper formatting is required for ConnectBot SSH (server bookmark field requires username@server).

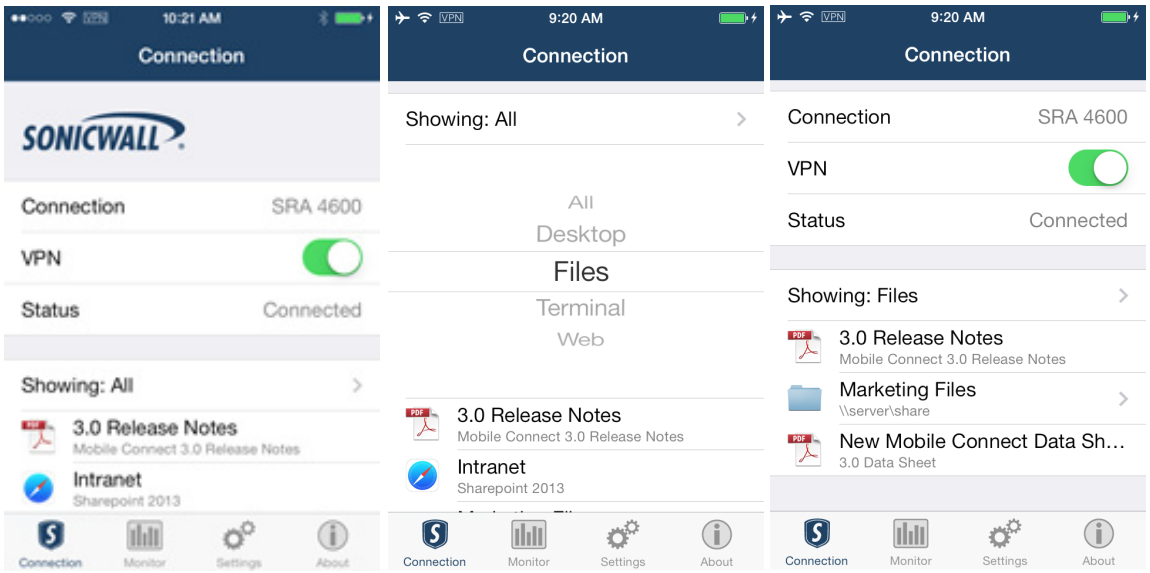
Files

Mobile Connect 3.0 introduces secure mobile access to files through new File bookmarks. File bookmarks allow secure access to files by first checking and enforcing the server configured file policy, and then securely downloading and displaying the file within the Mobile Connect app,

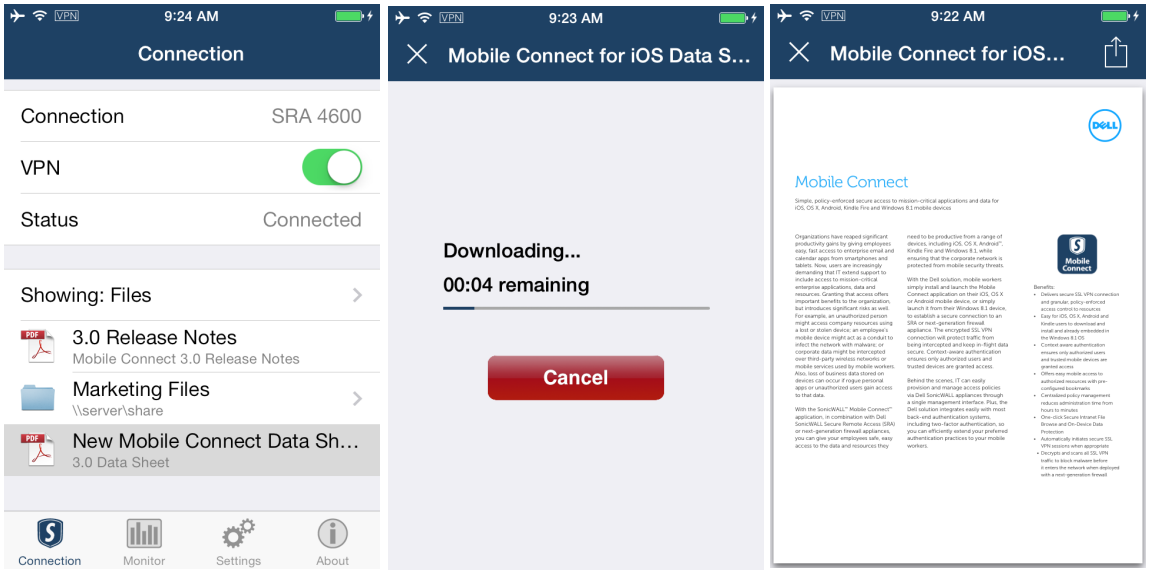
Server configured policies include control over whether a file may be printed, copied to the clipboard, opened in a third party app, or securely cached on the iOS device. File bookmarks can also be created to folders or file share root directories to allow directory navigation.

Note In Mobile Connect for iOS 3.0, File bookmarks are supported only on the Dell SonicWALL SRA appliances with SRA 7.5 or later firmware. Support for File bookmarks in E-Class SRA and Next Generation Firewall appliances is expected in a future release.

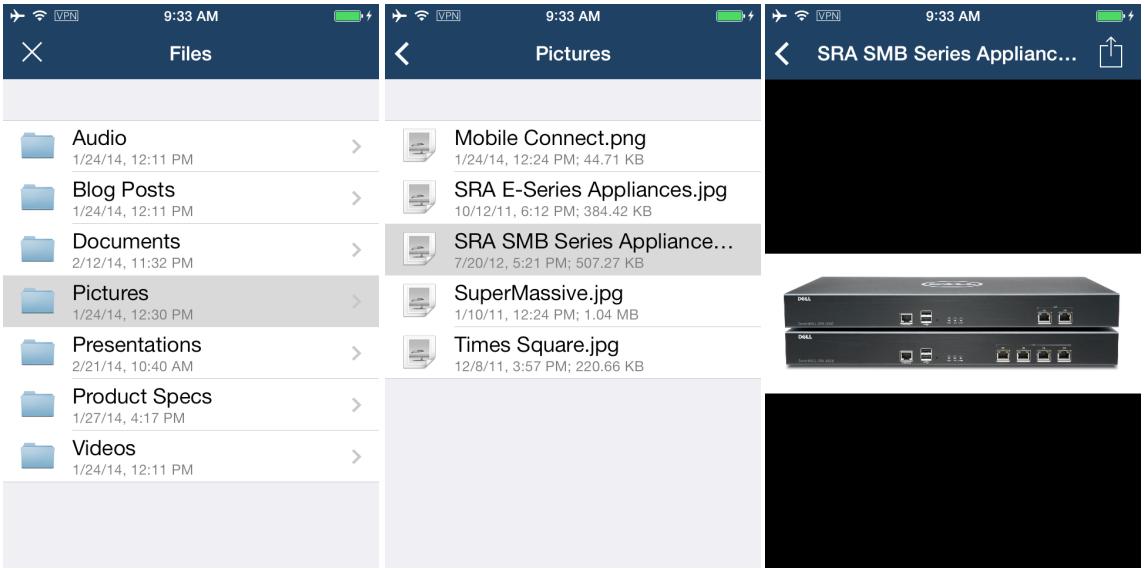
When File bookmarks are configured for the user on the server appliance, they appear in the list of bookmarks after the VPN is established and can be filtered by selecting the **Showing: Files** row that is displayed when there are more than five bookmarks.



Selecting a File bookmark queries the server and enforces any file policies configured on the server for that File bookmark. If the file is not already cached on the device, the file is securely downloaded from the SRA appliance. Once downloaded the file is displayed within the Mobile Connect app.



Selecting a File bookmark to a folder or directory allows directory browsing and download and viewing of any file in the folder. All attempts to browse a file folder or view a file will query the server to enforce access policies.



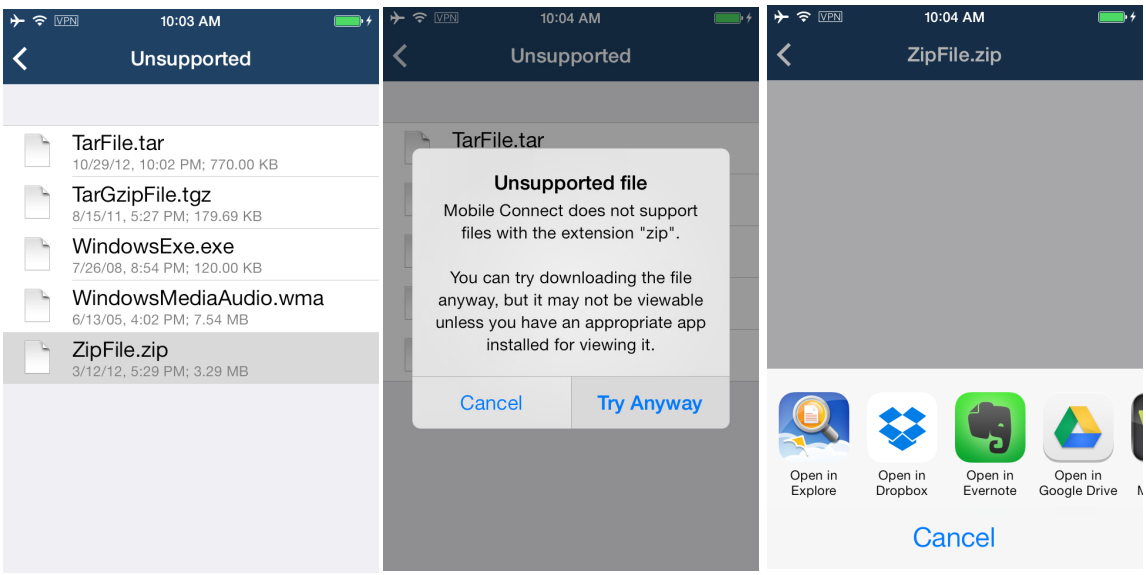
Supported File Types

Mobile Connect supports the file types natively supported by Apple iOS, including the following:

File Type	File Extension
Images	.jpg, .jpeg, .tif, .tiff, .png
Music	.mp3, .m4a, .wav
Movies	.mov, .mp4
Microsoft Word Documents	.doc, .docx
Microsoft Excel Spreadsheets	.xls, .xlsx
Microsoft PowerPoint Presentations	.ppt, .pptx
Adobe PDF	.pdf
Keynote Presentations	.key
Pages Documents	.pages
Numbers Spreadsheets	.numbers
Web Pages	.htm, .html
Text and Rich-text Files	.txt, .rtf

Unsupported File Types

If a file type is not supported, an Unsupported File message is displayed identifying that the file may not be viewable unless another app is installed that can view the file. Tap **Try Anyway** to try opening the file with another app that may be registered to handle that file type.

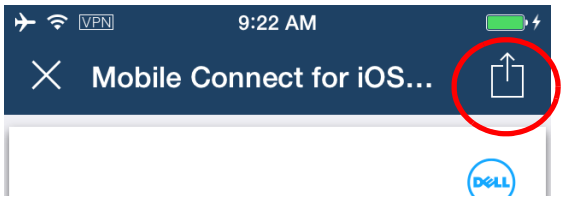


File Policies

On iOS, policies can be configured on the server to control whether a file may be:

- Printed,
- Copied to the clipboard,
- Opened in a third-party app, or
- Securely cached on the device.

If a file has an Allow policy (Allow Print, Allow Copy, or Allow Open In) enabled, a Share button is displayed in the top right of the navigation bar when the file is viewed:

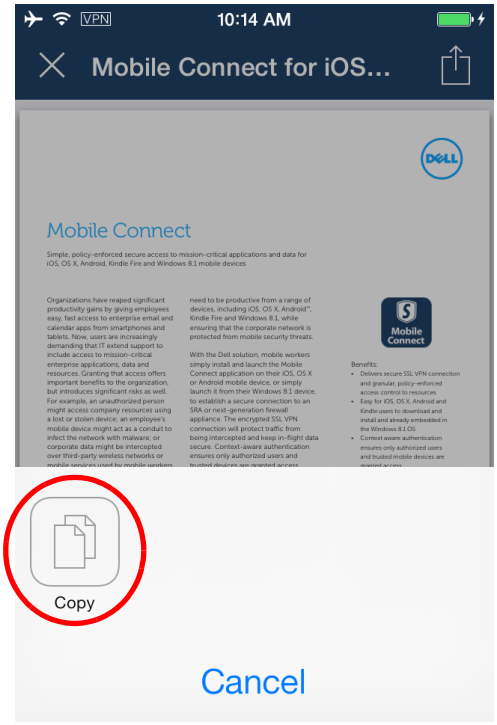


Allow Print

If the file has the Allow Print policy enabled, tapping the Share button displays the Print button.

Allow Copy

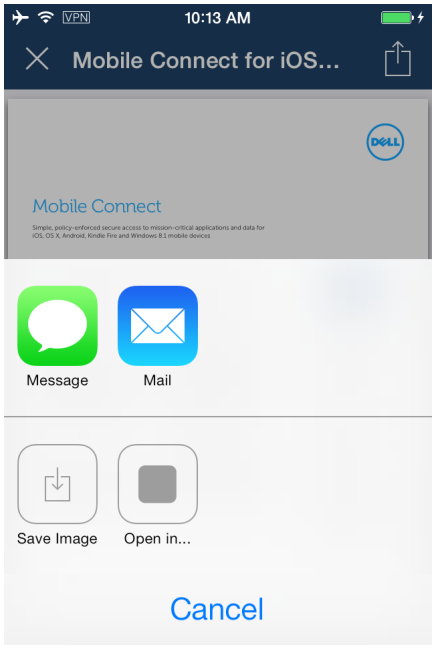
If the file has the Allow Copy policy enabled, tapping the Share button displays the Copy button.



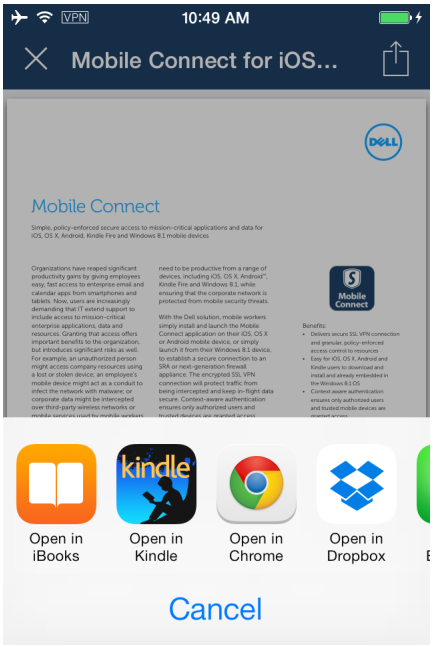
Allow Open In

If the file has the Allow Open in policy enabled, tapping the Share button displays the **Open in…** button and icons for other apps that can open the file.

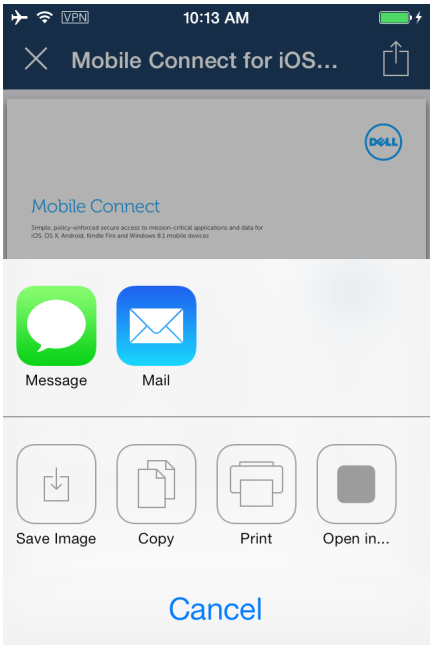
Tapping the **Open in…** button displays a list of apps that can open the file.



Tapping **Share** button



Tapping **Open In** button



Tapping **Share** button when all Files policies are enabled

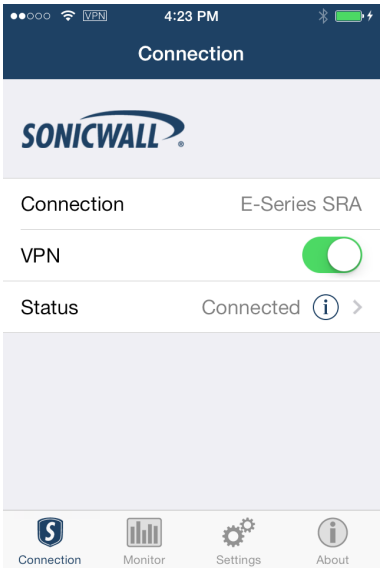
Configure Connect on Demand

Note Connect on Demand is only available for connections to Dell SonicWALL E-Class SRA and SMB SRA appliances.

The Connect on Demand feature provides the ability for Mobile Connect to automatically establish a VPN connection when you attempt to access a domain on the private network. This provides a seamless VPN connectivity experience without the need to manually launch Mobile Connect.

Configuring a Connection to Dell SonicWALL E-Class SRA Appliances

The easiest way to determine if Connect on Demand is available for your E-Class SRA connection is to look at the Connection tab when a VPN is connected. If the ⓘ › info indicator appears to the right of the Status row, Connect on Demand may be configured while connected.

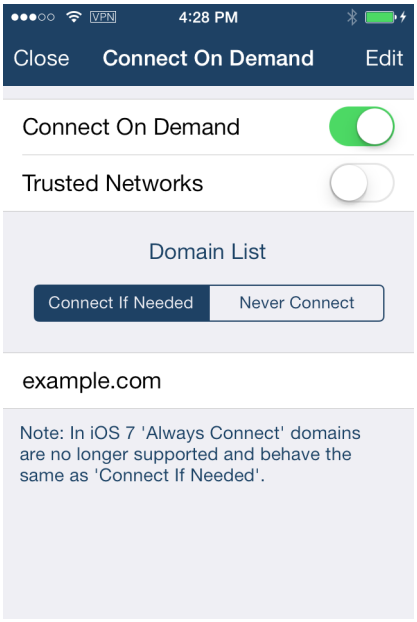


A VPN configuration on the Dell SonicWALL E-Class SRA appliance must meet the following requirements to support Connect on Demand.

- The VPN tunnel must not be configured for Redirect-All mode.
- The realm must be configured to use client certificates for authentication. Chained authentication (where a second authentication server is used) does not support Connect on Demand.
- The valid client certificate for the realm must be present.
- The user must successfully connect to the appliance at least once.

To configure Connect on Demand, perform the following tasks:

1. Tap the info indicator ⓘ ›in the Status row on the Connection tab, which displays the Connect On Demand screen.

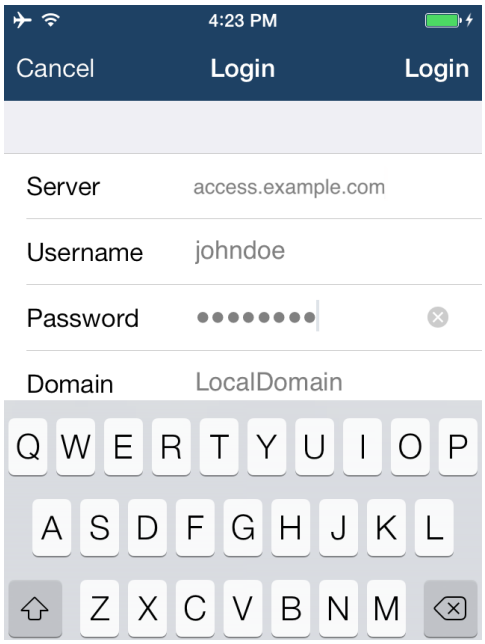


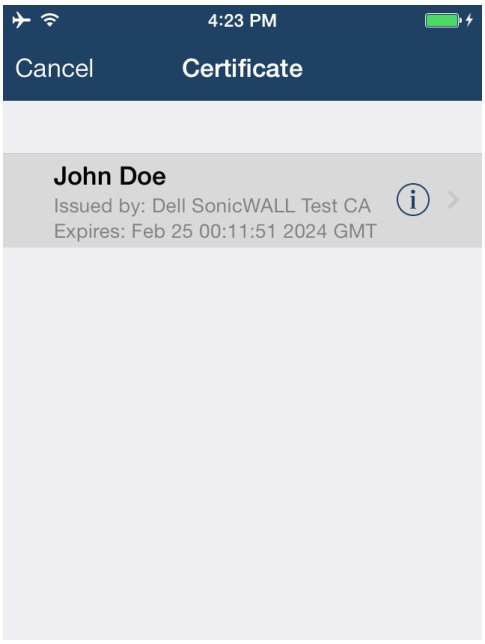
2. Tap **Connect on Demand**.
3. Set the **Domain List** option to **Connect If Needed** to have Mobile Connect establish a VPN connection when accessing a resource with any of the domain suffixes listed.
4. Setting the **Domain List** option to **Never Connect** disables Connect on Demand for the domain suffixes listed.
5. If more than one domain is listed, you can enable Connect on Demand for individual domains by tapping on the domain name.

Note In iOS 7 **Always Connect** domains are no longer supported and behave the same as **Connect if Needed**.

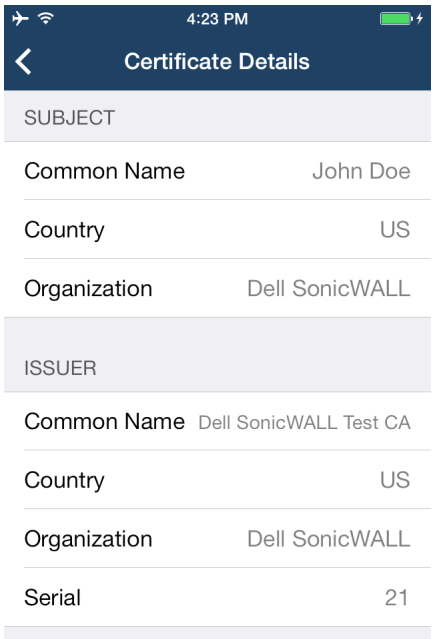
Configuring a Connection to Dell SonicWALL SMB SRA Appliances

On SMB SRA appliances, client certificate authentication is available as a second factor authentication method in addition to standard user name and password authentication. If a client certificate is required during authentication, the user is automatically prompted to select a client certificate from the iOS device.





Tapping on the info indicator ⓘ › that appears to the right of the client certificate displays additional details for the client certificate.

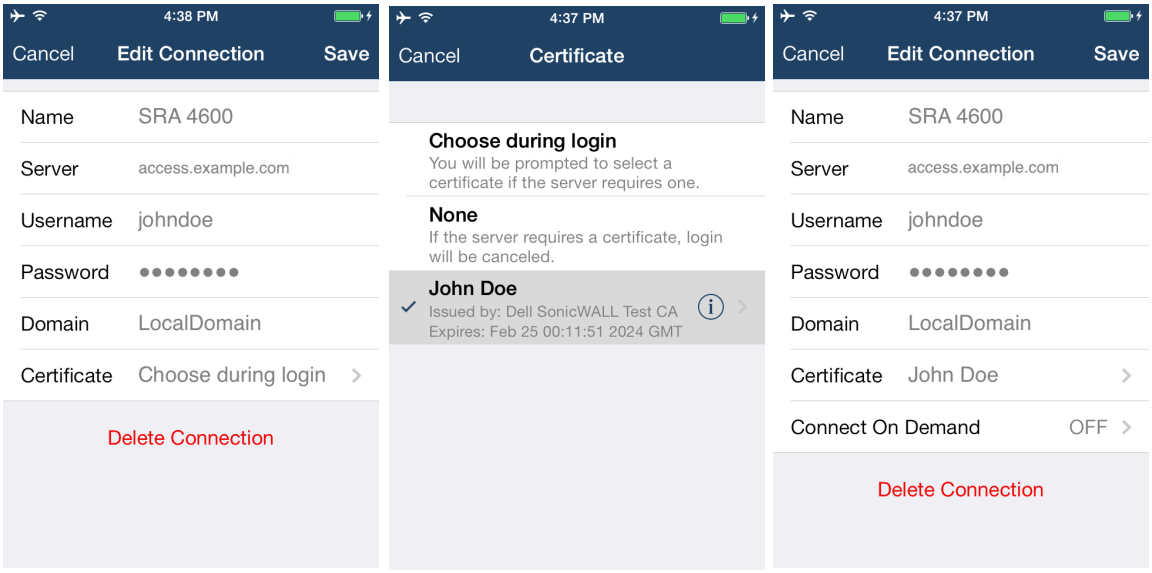


By default a VPN configuration will be the client certificate setting to **Choose during login**. To support Connect on Demand, a VPN connection should not request any user interaction to seamlessly connect. A VPN configuration on the Dell SonicWALL SMB SRA appliance must meet the following requirements:

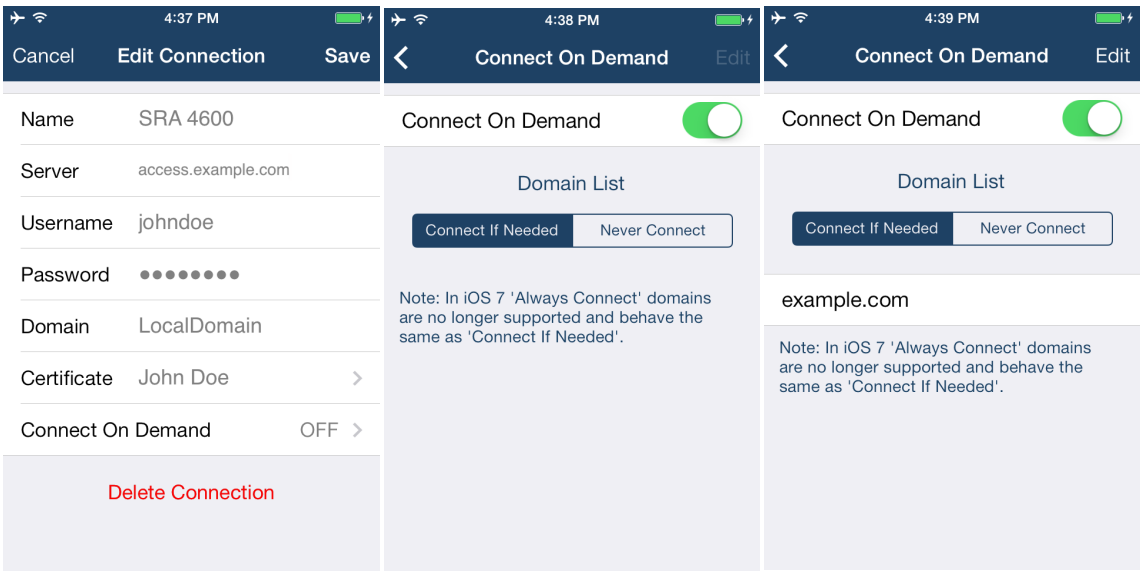
- The user's effective client certificate enforcement policy, configured at the domain or user level, must be enabled to use client certificates for authentication.
- The user's effective user name and password caching policy (configured at the global, group, or user level) must be set to **Allow saving of username and password**.
- The valid client certificate for the user must be present on the iOS device.
- The iOS VPN connection profile must have the user name and password configured, and the appropriate client certificate must be selected.

To configure Connect on Demand, perform the following tasks:

1. Select a client certificate under the Certificate row on the Edit Connection screen, which displays the Connect On Demand row:



2. Select the Connect On Demand row on the Edit Connection screen and enable Connect On Demand.

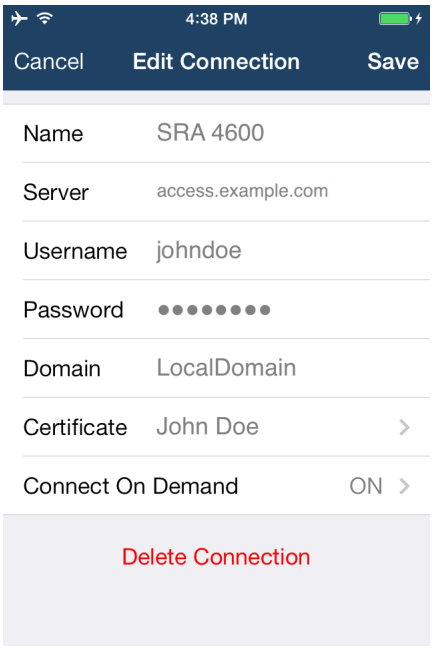


3. Set the **Domain List** option to **Connect If Needed** to have Mobile Connect establish a VPN connection when accessing a resource with any of the domain suffixes listed.

   Setting the **Domain List** option to **Never Connect** disables Connect on Demand for the domain suffixes listed.

4. If more than one domain is listed, tap a domain name to enable Connect on Demand for an individual domain.

Note In iOS 7 **Always Connect** domains are no longer supported and behave the same as **Connect if Needed**.



Configure Trusted Network Detection

The Apple Trusted Network Detection (TND) enhancement to the iOS Connect On Demand feature is available in iOS 6. TND results in the following:

- Can be used only with Connect on Demand.
- Extends the Connect on Demand functionality by determining whether the user is on a trusted network.
- Configured with the iPhone Configuration Utility.
- Used for Wi-Fi connections only. When operating over other types of network connections, Connect on Demand does not use TND to determine whether a VPN should be connected.

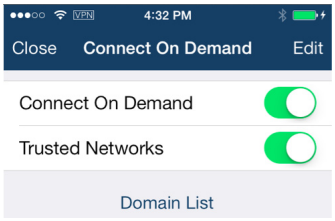
Connect On Demand starts a VPN connection whenever a user tries to access a destination with a hostname specified in the domains list. For example, if *.example.com is in the Always Connected list, when a user accesses internal.example.com, the client starts a VPN connection

regardless of the network to which the device is currently connected. TND compares the VPN and local DNS servers and DNS suffixes to determine whether to use Mobile Connect and dial the VPN, as shown in the following table:

DNS Suffixes	DNS Servers	Login
None	None	Refused - no VPN
None	Same	Refused - no VPN
Same	Same	Refused - no VPN
Same	Same and others	Allowed
Same	Different	Allowed
Different	Same	Allowed
Some	Some	Allowed

Consult documentation from Apple Inc. for more information about Trusted Network Detection and Connect on Demand.

To determine if TND is available for your connection, tap the info indicator in the Status row on the Connection tab. This displays the buttons used to enable/disable TND if available.



To configure TND, perform the following tasks:

1. Tap the info indicator ⓘ › in the Status row on the Connection tab.
2. Ensure Connect On Demand is turned on.
3. Turn on **Trusted Networks**.

Note **Trusted Network Detection** is available only for connections to Dell SonicWALL E-Class SRA appliances.

To Use the iPhone Configuration Utility with Mobile Connect

The iPhone Configuration Utility provides the ability for administrators of enterprise environments to create configuration profiles for the iPhone, iPod touch, and iPad. These profiles provide the ability for administrators to preconfigure the device settings for enterprise policies, such as VPN configuration, security policies, Wi-Fi settings, etc.

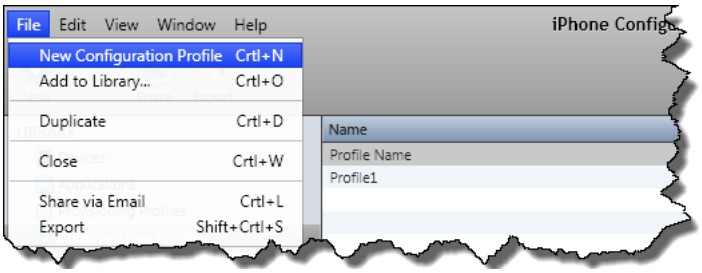
The iPhone Configuration Utility enables administrators to configure Mobile Connect profiles for their users' iOS devices. The iPhone Configuration Utility can be downloaded here:

http://www.apple.com/support/iphone/enterprise/

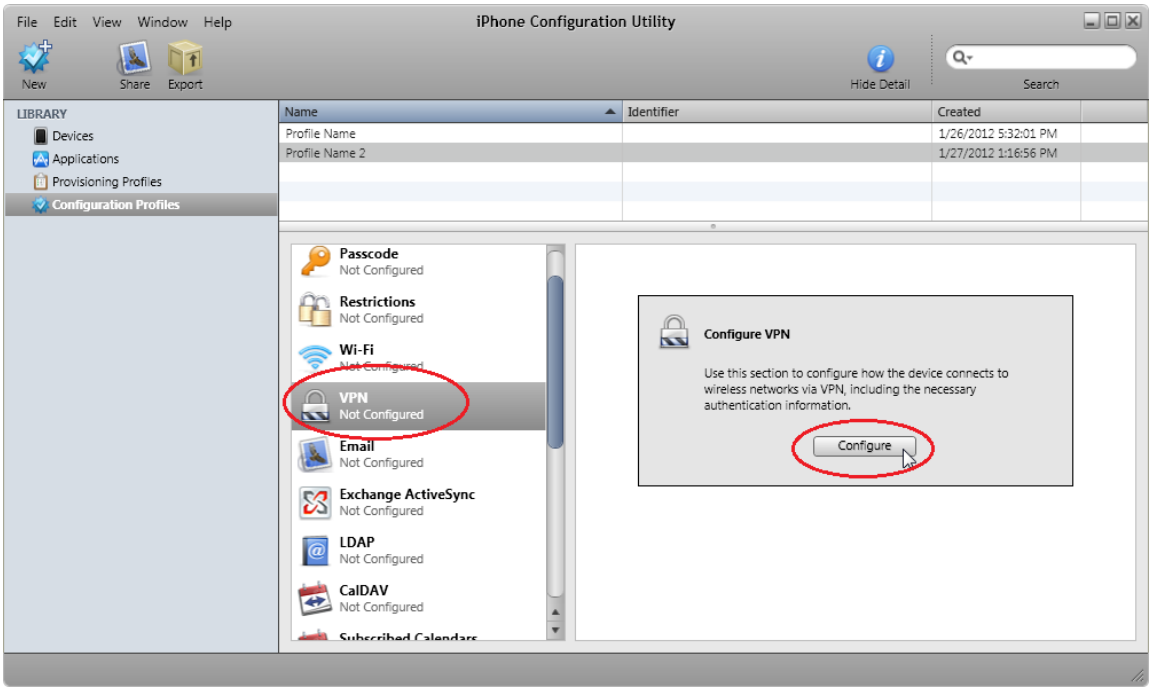
To configure a Mobile Connect profile using the iPhone Configuration Utility, perform the following steps.

1. Download, install and launch the iPhone Configuration Utility for Windows or Mac OS. X

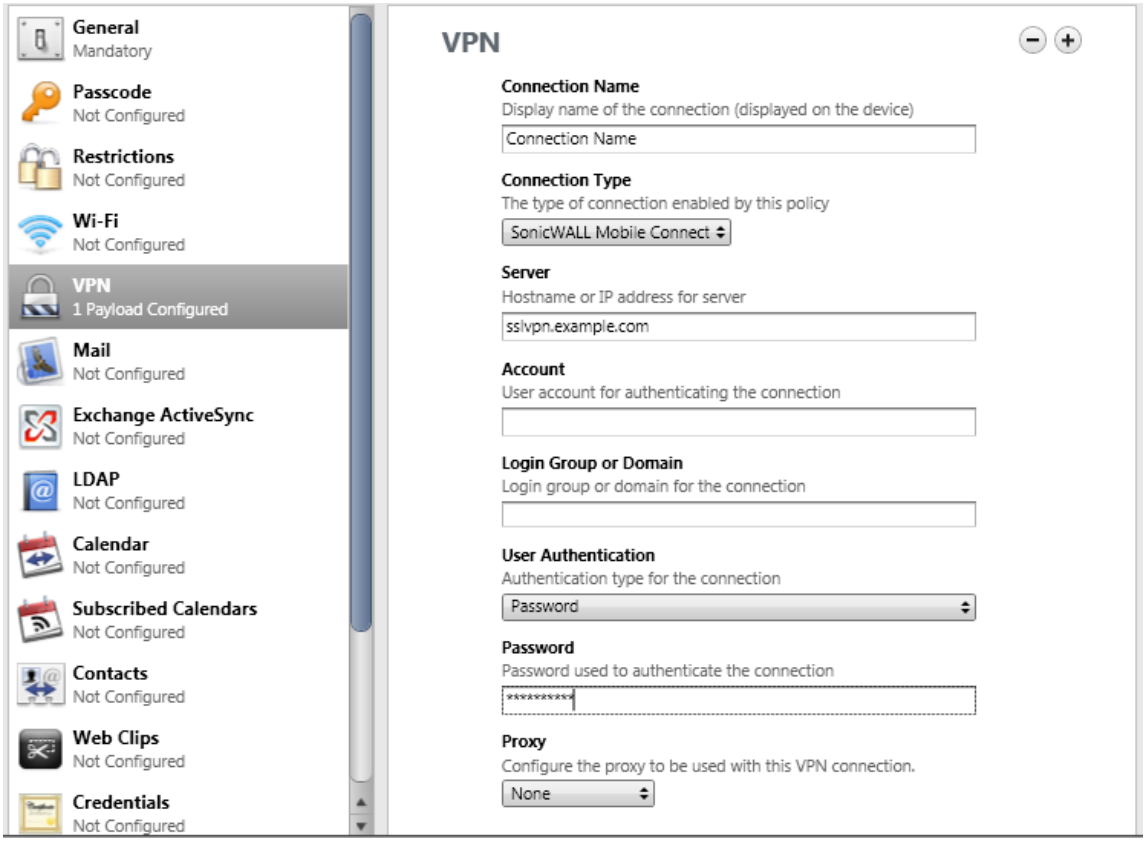
2. Click **File > New Configuration Profile**.



3. Select **VPN**, and then click the **Configure** button.



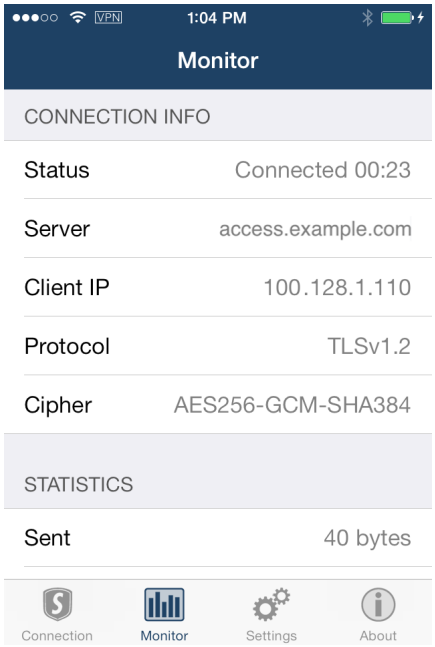
4. In the **Connection Name** field, enter **Connection Name**.



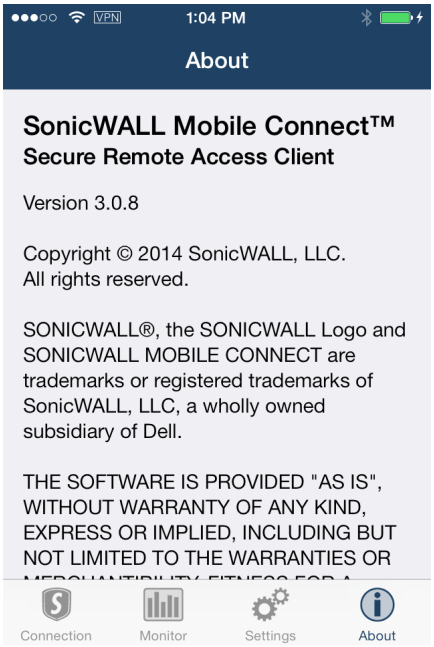
5. In the **Connection Type** drop-down menu, select **SonicWALL Mobile Connect**.
6. In the **Server** field, enter the hostname or IP address for the Dell SonicWALL appliance.
7. (Optional) In the **Account** field, enter the username for the account.
8. The Login Group or Domain value depends on the type of appliance used for the connection:
   - For profiles connecting to Dell SonicWALL UTM or SRA appliances, enter the value in the **Domain** field shown in the Edit Connection window of the Mobile Connect app.
   - For profiles connecting to Dell SonicWALL E-Class SRA appliances, enter the **v**alue selected in the **Log in to** window, when initiating a connection in Mobile Connect.
9. In the **User Authentication** drop-down menu, select **Password**.
10. (Optional for connections to UTM or SRA appliances) In the **Password** field, enter the password for the user account, if the Dell SonicWALL appliance you are connecting to is configured to allow for saving passwords. Note that only Dell SonicWALL UTM or SRA appliances can store passwords. Dell SonicWALL E-Class SRA appliances cannot allow for stored passwords.
11. (Optional for connections to E-Class SRA appliances) If a proxy server is used for the connect, in the **Proxy** drop-down menu, select either **Manual** or **Automatic**. If a proxy server is not used, leave this set to **None**. Note that only Dell SonicWALL E-Class SRA appliances support Mobile Connect over proxy. Currently, Dell SonicWALL UTM and SRA appliances do not support Mobile Connect over proxy.

Monitor Mobile Connect

The **Monitor** tab displays additional details about the connection, statistics on traffic transmitted, DNS information, and routes that have been installed.



The **About** tab of Mobile Connect displays the version number and legal text.


1:04 PM
About
SonicWALL Mobile Connect™
Secure Remote Access Client
Version 3.0.8
Copyright © 2014 SonicWALL, LLC.
All rights reserved.
SONICWALL®, the SONICWALL Logo and SONICWALL MOBILE CONNECT are trademarks or registered trademarks of SonicWALL, LLC, a wholly owned subsidiary of Dell.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OR
Connection
Monitor
Settings
About

Troubleshoot Mobile Connect

If you are unable to connect to the Dell SonicWALL server, perform the following steps to troubleshoot the connection.

1. Double check that you have entered the server name properly in the connection configuration.
2. Go to the Safari browser on your iPhone, iPod touch, or iPad and attempt to navigate to the SRA appliance web portal.
3. If you are unable to load the web portal, the problem is with the Dell SonicWALL appliance. Contact your network administrator if the problem persists.
4. If the web portal loads successfully on the Safari browser and you still cannot establish a Mobile Connect connection, notify Dell SonicWALL Support, as follows:
   a. On the **Settings** tab, enable the **Debug Logging** option.
   b. Attempt a connection to the server again to ensure that full debugging messages are logged for the attempt.
   c. Then return to the **Settings** tab and tap the **Email Logs** button. An email will launch in your mail client with the Mobile Connect log attached. Address the email to **Support@sonicwall.com**. Add any additional comments to the email and tap **Send**. Dell SonicWALL Support staff will contact you after reviewing your case.